JOURNAL OF NUMBER THEORY 38, 118–133 (1991)

On an Assertion of Ramanujan Concerning Binary Quadratic Forms

KENNETH S. WILLIAMS*

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada

Communicated by Hans Zassenhaus

Received February 21, 1990; revised May 1, 1990

The assertion concerning binary quadratic forms made by Ramanujan ("Notebook," Vol. 2, p. 311, Tata Institute of Fundamental Research, Bombay, 1957) is proved.

1. INTRODUCTION

In Ramanujan's notebook [7, Vol. 2, p. 311] is the statement

> "if a prime number of the form $An+B$ can be expressed as ax^2-by^2, then a prime number of the form $An-B$ can be expressed as bx^2-ay^2."

In a letter to the author [1], Bruce Berndt asked if this statement is true. After some preliminary results in Section 2 concerning the genera of classes of binary quadratic forms, we prove the following precise form of Ramanujan's assertion in Section 3. The author is grateful to Professor Berndt for stimulating his interest in Ramanujan's claim.

THEOREM. *Let a, b, A, B be positive integers satisfying*

$$GCD(a, b) = GCD(A, B) = 1, \qquad ab \neq \text{square},$$

which have the following property:

(*) *Every prime $p \equiv B \pmod{A}$ with $GCD(p, 2ab) = 1$ is expressible in the form ax^2-by^2 for some integers x and y.*

* Research supported by Grant A-7233 of the Natural Sciences and Engineering Research Council of Canada.

0022-314X/91 $3.00

Then every prime q satisfying

$$q \equiv -B \pmod{A}, \qquad GCD(q, 2ab) = 1$$

is expressible in the form $bX^2 - aY^2$ for some integers X and Y.

EXAMPLE 1. It is well known [6, p. 210] that every prime $p \equiv 1 \pmod 8$ is expressible in the form $x^2 - 2y^2$ (for example, $17 = 5^2 - 2.2^2$, $41 = 7^2 - 2.2^2$, $73 = 9^2 - 2.2^2$, $89 = 11^2 - 2.4^2$). The theorem guarantees that every prime $q \equiv -1 \pmod 8$ is expressible in the form $2X^2 - Y^2$. Since $2X^2 - Y^2 = (2X + Y)^2 - 2(X + Y)^2$ every prime $q \equiv 7 \pmod 8$ is also expressible in the form $x^2 - 2y^2$ (for example, $7 = 3^2 - 2.1^2$, $23 = 5^2 - 2.1^2$, $31 = 7^2 - 2.3^2$).

EXAMPLE 2. It is well known [6, p. 211] that every prime $p \equiv 1 \pmod{12}$ is expressible in the form $x^2 - 3y^2$ (for example, $13 = 4^2 - 3.1^2$, $37 = 7^2 - 3.2^2$, $61 = 8^2 - 3.1^2$). Hence, by the theorem, every prime $q \equiv -1 \pmod{12}$ is expressible in the form $3X^2 - Y^2$ (for example, $11 = 3.2^2 - 1^2$, $23 = 3.3^2 - 2^2$, $47 = 3.4^2 - 1^2$).

Suppose that a, b, A, B are positive integers satisfying $GCD(a, b) = GCD(A, B) = 1$, $ab \neq$ square, which have property (*). It follows from Corollary 2 in Section 2 that either

(a) $ab \equiv 0, 3, 4, 6, 7 \pmod 8$, or

(b) $ab \equiv 1, 2, 5 \pmod 8$ and ab possesses a prime divisor $\equiv 3 \pmod 4$, or

(c) $ab \equiv 1, 2, 5 \pmod 8$, every odd prime divisor of ab is $\equiv 1 \pmod 4$, and the equation $T^2 - abU^2 = -1$ is solvable in integers T and U.

We note that if (a) or (b) holds then $T^2 - abU^2 = -1$ is not solvable in integers T and U. If (a) or (b) holds, it is shown that a prime $q \equiv -B \pmod A$, $GCD(q, 2ab) = 1$, is expressible in the form $bX^2 - aY^2$ but not by $aX^2 - bY^2$, whereas if (c) holds every such prime q is represented by both $aX^2 - bY^2$ and $bX^2 - aY^2$. Some of these remarks have been observed by Berndt [1].

EXAMPLE 3. $a = 1$, $b = 7$, $A = 28$, $B = 9$ (type (a)) have property (*) as $p \equiv 9 \pmod{28}$ implies that $p = x^2 - 7y^2$ for integers x and y [5, Table III] (for example, $37 = 10^2 - 7.3^2$, $149 = 18^2 - 7.5^2$, $177 = 17^2 - 7.4^2$). Indeed every prime $q \equiv -9 \pmod{28}$ is expressible as $7X^2 - Y^2$ but not as $X^2 - 7Y^2$ (for example, $19 = 7.2^2 - 3^2$, $47 = 7.3^2 - 4^2$, $103 = 7.4^2 - 3^2$).

EXAMPLE 4. $a = 3$, $b = 7$, $A = 42$, $B = 17$ (type (b)) have property (*) as $p \equiv 17 \pmod{42}$ implies that $p = 3x^2 - 7y^2$ for some integers x and y [5,

Table III] (for example $17 = 3.8^2 - 7.5^2$, $59 = 3.13^2 - 7.8^2$, $101 = 3.6^2 - 7.1^2$). Thus every prime $q \equiv -17 \pmod{42}$ is expressible as $7X^2 - 3Y^2$ but not as $3X^2 - 7Y^2$ (for example, $67 = 7.5^2 - 3.6^2$, $109 = 7.4^2 - 3.1^2$).

EXAMPLE 5. $a = 5$, $b = 13$, $A = 65$, $B = 7$ (type (c)) have property $(*)$ as $p \equiv 7 \pmod{65}$ implies that $p = 5x^2 - 13y^2$ [5, Table III] (for example, $7 = 5.2^2 - 13.1^2$, $137 = 5.11^2 - 13.6^2$, $397 = 5.11^2 - 13.4^2$). Moreover every prime $q \equiv -7 \pmod{65}$ is expressible as both $5X^2 - 13Y^2$ and $13X^2 - 5Y^2$ (for example, $383 = 5.10^2 - 13.3^2 = 13.26^2 - 5.41^2$).

Example 6 below shows that the requirement in the theorem that *every* prime $p \equiv B \pmod{A}$, $GCD(p, 2ab) = 1$, be expressible in the form $ax^2 - by^2$ cannot be weakened to requiring only an *infinity* of such primes represented by $ax^2 - by^2$.

EXAMPLE 6. Infinitely many primes $p \equiv 1 \pmod{328}$ are expressible in the form $x^2 - 82y^2$ (for example $21977 = 165^2 - 82.8^2$, $25913 = 165^2 - 82.4^2$, $49201 = 247^2 - 82.12^2$), but not every prime $p \equiv 1 \pmod{328}$ is expressible as $x^2 - 82y^2$ (for example, $p = 2297$). Moreover, not every prime $q \equiv -1 \pmod{328}$ is expressible as $82X^2 - Y^2$ (for example, $q = 3607$). Theorems 5 and V of [4] with $r = 41$ give necessary and sufficient conditions for a prime p to be represented by $x^2 - 82y^2$.

2. PRELIMINARY RESULTS

If L, M, N are integers and x, y are independent variables, the function $f = f(x, y) = Lx^2 + Mxy + Ny^2$ is called an integral, binary quadratic form. If $GCD(L, M, N) = 1$, f is said to be primitive. A primitive, integral, binary quadratic form will just be called a form for short, and we will write (L, M, N) for the form $Lx^2 + Mxy + Ny^2$. The discriminant of the form (L, M, N) is the integer $M^2 - 4LN$. We consider throughout only those forms having discriminant $D = 4ab$, where a and b are positive coprime integers with ab nonsquare. The forms $(a, 0, -b) = ax^2 - by^2$ and $(b, 0, -a) = bx^2 - ay^2$, in which we are interested, both have discriminant $4ab$.

Two forms (L, M, N) and (L', M', N') of discriminant $D = 4ab$ are said to be equivalent, written $(L, M, N) \sim (L', M', N')$, if and only if there exist integers p, q, r, s with $ps - qr = 1$ such that

$$L(px + qy)^2 + M(px + qy)(rx + sy) + N(rx + sy)^2 = L'x^2 + M'xy + N'y^2.$$

The relation $\sim$ is an equivalence relation on the set of all forms of discriminant $D=4ab$. The equivalence classes are called form classes (of discriminant $D=4ab$). The class containing the form (L, M, N) is denoted by $[L, M, N]$. It is well known that the number $h(D)$ of form classes of discriminant D is finite.

A nonzero integer m is said to be represented by the form (L, M, N) if there exist integers x, y such that $m=Lx^2+Mxy+Ny^2$. The representation is called proper if $GCD(x, y)=1$. It is clear that forms in the same form class represent the same integers, so we can speak of a class representing an integer.

Next we recall the definition of the generic characters for the form classes of discriminant $D=4ab$. First we set

$$r=\text{number of distinct odd primes dividing } ab, \tag{2.1}$$

and

$$t=\begin{cases} r-1, & \text{if } ab\equiv 1, 5 \pmod 8,\\ r, & \text{if } ab\equiv 2, 3, 4, 6, 7 \pmod 8,\\ r+1, & \text{if } ab\equiv 0 \pmod 8. \end{cases} \tag{2.2}$$

We denote the r distinct odd primes dividing ab by $p_1, \ldots, p_r$. The $t+1$ generic characters $\chi_1, \ldots, \chi_{t+1}$ for the form classes of discriminant $D=4ab$ are defined as follows: for any integer m coprime with $2ab$

$$\chi_i(m)=\left(\frac{m}{p_i}\right) \qquad (i=1, 2, \ldots, t+1=r), \text{ if } ab\equiv 1, 5 \pmod 8; \tag{2.3}$$

$$\begin{cases} \chi_i(m)=\left(\dfrac{m}{p_i}\right) & (i=1, 2, \ldots, t=r),\\ \chi_{t+1}(m)=\left(\dfrac{2}{m}\right), & \text{if } ab\equiv 2 \pmod 8; \end{cases} \tag{2.4}$$

$$\begin{cases} \chi_i(m)=\left(\dfrac{m}{p_i}\right) & (i=1, 2, \ldots, t=r),\\ \chi_{t+1}(m)=\left(\dfrac{-1}{m}\right), & \text{if } ab\equiv 3, 4, 7 \pmod 8; \end{cases} \tag{2.5}$$

$$\begin{cases} \chi_i(m)=\left(\dfrac{m}{p_i}\right) & (i=1, 2, \ldots, t=r),\\ \chi_{t+1}(m)=\left(\dfrac{-2}{m}\right), & \text{if } ab\equiv 6 \pmod 8; \end{cases} \tag{2.6}$$

$$\begin{cases} \chi_i(m)=\left(\dfrac{m}{p_i}\right) & (i=1, 2, ..., t-1=r), \\ \chi_t(m)=\left(\dfrac{2}{m}\right), & \\ \chi_{t+1}(m)=\left(\dfrac{-1}{m}\right), & \text{if } ab\equiv 0 \pmod 8; \end{cases} \tag{2.7}$$

where (m/p_i) is the Legendre symbol of quadratic residuacity (mod p_i) and

$$\left(\frac{-1}{m}\right)=\left\{\begin{matrix} 1, & \text{if } m\equiv 1 \pmod 4 \\ -1, & \text{if } m\equiv 3 \pmod 4 \end{matrix}\right\},$$

$$\left(\frac{2}{m}\right)=\left\{\begin{matrix} 1, & \text{if } m\equiv 1, 7 \pmod 8 \\ -1, & \text{if } m\equiv 3, 5 \pmod 8 \end{matrix}\right\},$$

$$\left(\frac{-2}{m}\right)=\left\{\begin{matrix} 1, & \text{if } m\equiv 1, 3 \pmod 8 \\ -1, & \text{if } m\equiv 5, 7 \pmod 8 \end{matrix}\right\},$$

see, for example, [3]. The generic characters $(-1/m)$, $(2/m)$, $(-2/m)$ are often called supplementary characters.

If m and m' are two different integers, both coprime with $2ab$, which are represented by the form class $[L, M, N]$ of discriminant $4ab$, then $\chi_i(m)=\chi_i(m')$ $(i=1, 2, ..., t+1)$. Thus we may partition the set of form classes of discriminant $4ab$ into 2^{t+1} subsets

$$\begin{aligned} \{\delta_1, ..., \delta_{t+1}\} = \{&\text{form classes } C \text{ of discriminant } 4ab \text{ such} \\ &\text{that } \chi_i(m)=\delta_i (i=1, ..., t+1) \text{ for some integer} \\ &m \text{ coprime with } 2ab \text{ represented by the class } C\}, \end{aligned} \tag{2.8}$$

where each $\delta_i=\pm 1$ $(i=1, ..., t+1)$. A *nonempty* set $\{\delta_1, ..., \delta_{t+1}\}$ is called a genus (plural: genera). Gauss proved that there are exactly 2^t genera and that each genus contains exactly $h(4ab)/2^t$ form classes. The genera for discriminant $D=4ab$ can be determined by means of the product rule. In order to state the product rule we must introduce a little more notation. For each $i=1, ..., r$ we let $p_i^{d_i}$ denote the exact power of p_i dividing ab so that $d_i\geqslant 1$ $(i=1, ..., r)$. We also let 2^d denote the exact power of 2 dividing ab and set $E=ab/2^d$, so that $E\equiv 1 \pmod 2$. We also define e_i for $i=1, ..., t+1$ as follows:

$$\text{for } i=1, ..., r \qquad e_i=\begin{cases} 0, & \text{if } d_i\equiv 0 \pmod 2, \\ 1, & \text{if } d_i\equiv 1 \pmod 2; \end{cases} \tag{2.9}$$

$$\text{if } ab \equiv 2 \pmod 8 \qquad e_{t+1} = \begin{cases} 0, & \text{if } d \equiv 0 \pmod 2, \\ 1, & \text{if } d \equiv 1 \pmod 2; \end{cases} \tag{2.10}$$

$$\text{if } ab \equiv 3, 4, 7 \pmod 8 \qquad e_{t+1} = \begin{cases} 0, & \text{if } E \equiv 1 \pmod 4, \\ 1, & \text{if } E \equiv 3 \pmod 4; \end{cases} \tag{2.11}$$

$$\text{if } ab \equiv 6 \pmod 8 \qquad e_{t+1} = 1; \tag{2.12}$$

$$\text{if } ab \equiv 0 \pmod 8 \qquad \begin{aligned} e_t &= \begin{cases} 0, & \text{if } d \equiv 0 \pmod 2, \\ 1, & \text{if } d \equiv 1 \pmod 2, \end{cases} \\ e_{t+1} &= \begin{cases} 0, & \text{if } E \equiv 1 \pmod 4, \\ 1, & \text{if } E \equiv 3 \pmod 4. \end{cases} \end{aligned} \tag{2.13}$$

The product rules asserts

$$\prod_{i=1}^{t+1} \chi_i^{e_i}(m) = 1, \qquad \text{if } GCD(m, 2ab) = 1, \left(\frac{ab}{m}\right) = 1. \tag{2.14}$$

EXAMPLE 7. $a = 2$, $b = 41$. Here $ab = 82 \equiv 2 \pmod 8$, $t = r = 1$. There are $t + 1 = 2$ generic characters, namely, $\chi_1(m) = (m/41)$ and $\chi_2(m) = (2/m)$. The product rule gives $\chi_1(m)\chi_2(m) = 1$, if $GCD(m, 82) = 1$, $(82/m) = 1$. There are $h(328) = 4$ form classes, namely, $[1, 0, -82]$, $[2, 0, -41]$, $[3, 2, -27]$, $[3, -2, -27]$ and these fall into $2^t = 2$ genera as follows

$$\{+1, +1\} = \{[1, 0, -82], [2, 0, -41]\},$$
$$\{-1, -1\} = \{[3, 2, -27], [3, -2, -27]\}.$$

If m is an integer such that $(m/41) = (2/m) = -1$ then m is represented by the form $(3, 2, -27)$. If m is an integer such that $(m/41) = (2/m) = 1$ then m is represented by at least one of the two forms $(1, 0, -82)$, $(2, 0, -41)$ and additional information regarding m is needed before it can be determined exactly which of these represents m. For example $m = -319$ is represented by both of them as $-319 = 3^2 - 82.2^2 = 2.5^2 - 41.3^2$, whereas -1 is represented by $(1, 0, -82)(-1 = 9^2 - 82.1^2)$ but not by $(2, 0, -41)$. However, when p is a prime such that $(p/41) = (2/p) = 1$, then p is represented by exactly one of the forms $(1, 0, -82)$, $(2, 0, -41)$. Kaplan, Williams, and Yamamoto [4, Theorems 5, V with $r = 41$] have shown

$$p = X^2 - 82Y^2, \qquad \text{if } \left(\frac{a + 17b}{41}\right) = +1,$$

$$p = 2X^2 - 41Y^2, \qquad \text{if } \left(\frac{a + 17b}{41}\right) = -1,$$

where a and b are positive integers such that $p = a^2 - 2b^2$.

We are now ready to give the preliminary results we shall need in order to prove the theorem. It is convenient to set for $i = 1, ..., r$

$$\theta_i = \begin{cases} 0, & \text{if } p_i \equiv 1 \pmod 4, \\ 1, & \text{if } p_i \equiv 3 \pmod 4, \end{cases} \tag{2.15}$$

so that $p_i \equiv (-1)^{\theta_i} \pmod 4$ and $\chi_i(-1) = (-1/p_i) = (-1)^{\theta_i}$.

LEMMA 1. *If the form class* $[a, 0, -b]$ *belongs to the genus* $\{\delta_1, ..., \delta_{t+1}\}$ *then the form class* $[-a, 0, b]$ *belongs to the genus*

(i) $\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_{t+1}}\delta_{t+1}\}$, *if* $ab \equiv 1, 5 \pmod 8$,

(ii) $\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_t}\delta_t, \delta_{t+1}\}$, *if* $ab \equiv 2 \pmod 8$,

(iii) $\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_t}\delta_t, -\delta_{t+1}\}$, *if* $ab \equiv 3, 4, 6, 7 \pmod 8$,

(iv) $\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_{t-1}}\delta_{t-1}, \delta_t, -\delta_{t+1}\}$, *if* $ab \equiv 0 \pmod 8$.

Proof. Let m be an integer coprime with $2ab$ which is represented by the class $[-a, 0, b]$. Then there exist integers x and y such that $m = -ax^2 + by^2$. Clearly $-m = ax^2 - by^2$ so that $-m$ is represented by the form class $[a, 0, -b]$. As the form class $[a, 0, -b]$ belongs to the genus $\{\delta_1, ..., \delta_{t+1}\}$, we have

$$\chi_i(-m) = \delta_i \qquad (i = 1, 2, ..., t+1).$$

Thus, for $i = 1, ..., r$, we have

$$\chi_i(m) = \chi_i(-1)\,\chi_i(-m) = (-1)^{\theta_i}\delta_i.$$

Next we determine $\chi_i(m)$ $(i = r+1, ..., t+1)$. We consider cases depending on $ab \pmod 8$.

(i) $ab \equiv 1, 5 \pmod 8$. Here $r = t+1$ and there are no supplementary characters. Thus $[-a, 0, b]$ belongs to the genus $\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_{t+1}}\delta_{t+1}\}$.

(ii) $ab \equiv 2 \pmod 8$. Here $r = t$ and there is one additional generic character χ_{t+1} to consider. We have

$$\chi_{t+1}(m) = \left(\frac{2}{m}\right) = \left\{\begin{array}{ll} +1, & \text{if } m \equiv \pm 1 \pmod 8 \\ -1, & \text{if } m \equiv \pm 3 \pmod 8 \end{array}\right\}$$

$$= \left(\frac{2}{-m}\right) = \chi_{t+1}(-m) = \delta_{t+1},$$

so that $[-a, 0, b]$ belongs to the genus $\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_t}\delta_t, \delta_{t+1}\}$.

(iii) $ab \equiv 3, 4, 7 \pmod 8$. Here $r = t$ and there is one additional generic character χ_{t+1} to consider. We have

$$\chi_{t+1}(m) = \left(\frac{-1}{m}\right) = \left\{\begin{matrix} +1, & \text{if } m \equiv 1 \pmod 4 \\ -1, & \text{if } m \equiv 3 \pmod 4 \end{matrix}\right\}$$

$$= -\left(\frac{-1}{-m}\right) = -\chi_{t+1}(-m) = -\delta_{t+1},$$

so $[-a, 0, b]$ belongs to the genus $\{(-1)^{\theta_1}\delta_1, \ldots, (-1)^{\theta_t}\delta_t, -\delta_{t+1}\}$.

(iv) $ab \equiv 6 \pmod 8$. Here $r = t$ and there is one additional generic character χ_{t+1} to consider. We have

$$\chi_{t+1}(m) = \left(\frac{-2}{m}\right) = \left\{\begin{matrix} +1, & \text{if } m \equiv 1, 3 \pmod 8 \\ -1, & \text{if } m \equiv 5, 7 \pmod 8 \end{matrix}\right\}$$

$$= -\left(\frac{-2}{-m}\right) = -\chi_{t+1}(-m) = -\delta_{t+1},$$

so $[-a, 0, b]$ belongs to the genus $\{(-1)^{\theta_1}\delta_1, \ldots, (-1)^{\theta_t}\delta_t, -\delta_{t+1}\}$.

(v) $ab \equiv 0 \pmod 8$. Here $r = t-1$ and there are two additional generic characters to consider, namely $\chi_t(k) = (2/k)$, $\chi_{t+1}(k) = (-1/k)$. Exactly as above we have $\chi_t(m) = \delta_t$, $\chi_{t+1}(m) = -\delta_{t+1}$, so that $[-a, 0, b]$ belongs to the genus $\{(-1)^{\theta_1}\delta_1, \ldots, (-1)^{\theta_{t-1}}\delta_{t-1}, \delta_t, -\delta_{t+1}\}$.

This completes the proof of Lemma 1. ∎

LEMMA 2. *The form classes* $[a, 0, -b]$ *and* $[-a, 0, b]$ *belong to the same genus if and only if*

(i) $ab \equiv 1, 2, 5 \pmod 8$ *and*

(ii) *every odd prime dividing* ab *is* $\equiv 1 \pmod 4$.

Proof. It is clear from Lemma 1 that $[a, 0, -b]$ and $[-a, 0, b]$ cannot belong to the same genus if $ab \equiv 0, 3, 4, 6, 7 \pmod 8$. If $ab \equiv 1, 2, 5 \pmod 8$ they belong to the same genus if and only if $\theta_i = 0$ $(i = 1, \ldots, r)$, that is, if and only if all the odd prime factors of ab are $\equiv 1 \pmod 4$. This completes the proof of Lemma 2. ∎

LEMMA 3. *The form classes* $[a, 0, -b]$ *and* $[-a, 0, b]$ *are equal if and only if there are integers* T *and* U *such that* $T^2 - abU^2 = -1$.

Proof. The two forms $(a, 0, -b)$ and $(-a, 0, b)$ have the same discriminant $4ab$. Hence, by a well-known criterion (see, for example, [2,

Theorem 68]), they are equivalent if and only if there exist two integers α and γ such that

$$-a = a\alpha^2 - b\gamma^2,$$

$$2a\alpha \equiv 0 \pmod{2a},$$

$$2b\gamma \equiv 0 \pmod{2a}.$$

The first congruence holds trivially and the second congruence is equivalent to $\gamma \equiv 0 \pmod{a}$ as $GCD(a, b) = 1$. The solvability of the pair

$$-a = a\alpha^2 - b\gamma^2, \qquad \gamma \equiv 0 \pmod{a},$$

in integers α and γ is clearly equivalent to the solvability of the equation

$$T^2 - abU^2 = -1,$$

in integers T and U. This completes the proof of Lemma 3. ∎

Remark. It follows immediately from Lemmas 2 and 3 that

$$\left\{\begin{array}{c} T^2 - abU^2 = -1 \text{ solvable in} \\ \text{integers } T \text{ and } U \end{array}\right\}$$

$$\Rightarrow \left\{\begin{array}{c} ab \equiv 1, 2, 5 \pmod 8 \text{ and} \\ \text{every odd prime divisor of } ab \text{ is } \equiv 1 \pmod 4. \end{array}\right\} \tag{2.16}$$

The implication (2.16) is also easily proved directly.

COROLLARY 1. (i) $[a, 0, -b] = [-a, 0, b]$, *if* $T^2 - abU^2 = -1$ *is solvable,*

(ii) $[a, 0, -b]$, $[-a, 0, b]$ *are distinct but belong to the same genus, if* $T^2 - abU^2 = -1$ *is insolvable,* $ab \equiv 1, 2, 5 \pmod 8$, *and every odd prime divisor of* ab *is* $\equiv 1 \pmod 4$,

(iii) $[a, 0, -b]$, $[-a, 0, b]$ *belong to different genera, if either* $ab \equiv 0, 3, 4, 6, 7 \pmod 8$ *or* $ab \equiv 1, 2, 5 \pmod 8$ *and* ab *possesses a prime divisor* $\equiv 3 \pmod 4$.

Proof. This follows immediately from Lemmas 2 and 3. ∎

LEMMA 4. *Suppose that* a, b, A, B *are positive integers satisfying* $GCD(a, b) = GCD(A, B) = 1$, $ab \neq$ *square, which have property* (*). *Then, without loss of generality, we may suppose that* A *is even and* B *is odd, and, moreover, we have*

$$A \equiv 0 \pmod{2p_1 \cdots p_r}, \qquad \text{if} \quad ab \equiv 1, 5 \pmod 8,$$

$$A \equiv 0 \pmod{4p_1 \cdots p_r}, \qquad \text{if} \quad ab \equiv 3, 4, 7 \pmod 8,$$

$$A \equiv 0 \pmod{8p_1 \cdots p_r}, \qquad \text{if} \quad ab \equiv 0, 2, 6 \pmod 8.$$

Proof. Let p be an odd prime $\equiv B \pmod{A}$. As $GCD(A, B) = 1$ at least one of A and B is odd. If A and B are both odd we have $p \equiv B \pmod{2A}$. If A is odd and B is even we have $p \equiv A + B \pmod{2A}$. Hence, without loss of generality, we may suppose that A is even and B is odd.

We let $\{\delta_1, ..., \delta_{t+1}\}$ be the genus containing the form class $[a, 0, -b]$. We first show that $A \equiv 0 \pmod{p_1 \cdots p_r}$. Suppose that this is not the case. Then there is at least one integer i $(1 \leqslant i \leqslant r)$ with $p_i \nmid A$. Let k be an integer such that $(k/p_i) = -\delta_i$. Let M be an integer such that $Mp_i \equiv 1 \pmod{A}$ and N an integer such that $NA \equiv 1 \pmod{p_i}$. Then, as

$$\begin{aligned} &GCD(Mp_iB + NAk, Ap_i) \\ &\quad = GCD(Mp_iB + NAk, A)\, GCD(Mp_iB + NAk, p_i) \\ &\quad = GCD(Mp_iB, A)\, GCD(NAk, p_i) \\ &\quad = GCD(B, A)\, GCD(k, p_i) \\ &\quad = 1, \end{aligned}$$

by Dirichlet's theorem, there exist infinitely many primes $p \equiv Mp_iB + NAk \pmod{Ap_i}$. Choose one of these primes p so that $GCD(p, 2ab) = 1$. Clearly $p \equiv B \pmod{A}$, and, as a, b, A, B have property $(*)$, p must be represented by the form $(a, 0, -b)$. Since $[a, 0, -b]$ belongs to the genus $\{\delta_1, ..., \delta_{t+1}\}$ we have $\chi_j(p) = \delta_j$ $(j = 1, ..., t+1)$. Thus, in particular for $j = i$, we have (as $p \equiv k \pmod{p_i}$)

$$\delta_i = \chi_i(p) = \left(\frac{p}{p_i}\right) = \left(\frac{k}{p_i}\right) = -\delta_i,$$

which is impossible. Hence each p_i $(1 \leqslant i \leqslant r)$ divides A and so

$$A \equiv 0 \pmod{2p_1 p_2 \cdots p_r}.$$

To complete the proof of Lemma 4 we show that (a) $4 \mid A$ if $ab \equiv 3, 4, 7 \pmod{8}$ *and* (b) $8 \mid A$ if $ab \equiv 0, 2, 6 \pmod{8}$.

(a) $ab \equiv 3, 4, 7 \pmod{8}$. Suppose that $4 \nmid A$. As A is even we have $A \equiv 2 \pmod{4}$. Let k be an odd integer such that $(-1/k) = -\delta_{t+1}$. Then

$$\begin{aligned} &GCD\left((k - B)\left(\frac{A}{2}\right)^2 + B, 2A\right) \\ &\quad = GCD\left((k - B)\left(\frac{A}{2}\right)^2 + B, \frac{A}{2}\right) GCD\left((k - B)\left(\frac{A}{2}\right)^2 + B, 4\right) \\ &\quad = GCD\left(B, \frac{A}{2}\right) GCD(k, 4) \\ &\quad = 1, \end{aligned}$$

and so, by Dirichlet's theorem, there are infinitely many primes $p \equiv (k-B)(A/2)^2 + B \pmod{2A}$. Choose one of these so that $GCD(p, 2ab) = 1$. Clearly $p \equiv B \pmod{A/2}$ and, as p is odd, we have $p \equiv B \pmod{A}$. Thus, as a, b, A, B have property $(*)$, p must be represented by the form $(a, 0, -b)$. Since $[a, 0, -b]$ belongs to the genus $\{\delta_1, ..., \delta_{t+1}\}$ we have $\chi_j(p) = \delta_j$ $(j = 1, ..., t+1)$. Thus, in particular, for $j = t+1$, we have, as $p \equiv k \pmod 4$,

$$\delta_{t+1} = \chi_{t+1}(p) = \left(\frac{-1}{p}\right) = \left(\frac{-1}{k}\right) = -\delta_{t+1},$$

which is impossible. Hence $A \equiv 0 \pmod 4$ in this case.

(b) $ab \equiv 0, 2, 6 \pmod 8$. Suppose that $8 \nmid A$, so that (as A is even) we have (i) $A \equiv 2 \pmod 4$ or (ii) $A \equiv 4 \pmod 8$.

(i) $A \equiv 2 \pmod 4$. We let k be an odd integer such that

$$\left(\frac{-1}{k}\right) = -\delta_{t+1}, \qquad \text{if} \quad ab \equiv 0 \pmod 8,$$

$$\left(\frac{2}{k}\right) = -\delta_{t+1}, \qquad \text{if} \quad ab \equiv 2 \pmod 8,$$

$$\left(\frac{-2}{k}\right) = -\delta_{t+1}, \qquad \text{if} \quad ab \equiv 6 \pmod 8.$$

Next we note that

$$\begin{aligned} &GCD\left((k-B)\left(\frac{A}{2}\right)^2 + B, 4A\right) \\ &\quad = GCD\left((k-B)\left(\frac{A}{2}\right)^2 + B, 8\right) GCD\left((k-B)\left(\frac{A}{2}\right)^2 + B, \frac{A}{2}\right) \\ &\quad = GCD(k, 8)\, GCD(B, A/2) \\ &\quad = 1, \end{aligned}$$

so that there exist infinitely many primes $p \equiv (k-B)(A/2)^2 + B \pmod{4A}$. Choose one of these primes so that $GCD(p, 2ab) = 1$. Clearly we have $p \equiv B \pmod{A/2}$ and so, as p is odd, we have $p \equiv B \pmod{A}$. Thus, as a, b, A, B have property $(*)$, p is represented by the form $(a, 0, -b)$. As the form class $[a, 0, -b]$ belongs to the genus $\{\delta_1, ..., \delta_{t+1}\}$, we have $\chi_j(p) = \delta_j$ $(j = 1, ..., t+1)$. Thus, in particular, for $j = t+1$, we have (as $p \equiv k \pmod 8$))

$$\delta_{t+1} = \chi_{t+1}(p) = \begin{cases} \left(\frac{-1}{p}\right) = \left(\frac{-1}{k}\right) = -\delta_{t+1}, & \text{if } ab \equiv 0 \pmod 8, \\ \left(\frac{2}{p}\right) = \left(\frac{2}{k}\right) = -\delta_{t+1}, & \text{if } ab \equiv 2 \pmod 8, \\ \left(\frac{-2}{p}\right) = \left(\frac{-2}{k}\right) = -\delta_{t+1}, & \text{if } ab \equiv 6 \pmod 8, \end{cases}$$

which is impossible.

(ii) $A \equiv 4 \pmod 8$. We define an odd integer k as follows:
if $ab \equiv 0 \pmod 8$

$$k = \begin{cases} 1, & \text{if } B \equiv 1 \pmod 4,\ \delta_t \delta_{t+1} = -1, \\ 3, & \text{if } B \equiv 3 \pmod 4,\ \delta_t \delta_{t+1} = -1, \\ 5, & \text{if } B \equiv 1 \pmod 4,\ \delta_t \delta_{t+1} = 1, \\ 7, & \text{if } B \equiv 3 \pmod 4,\ \delta_t \delta_{i+1} = 1; \end{cases}$$

if $ab \equiv 2 \pmod 8$

$$k = \begin{cases} 1, & \text{if } B \equiv 1 \pmod 4,\ \delta_{t+1} = -1, \\ 3, & \text{if } B \equiv 3 \pmod 4,\ \delta_{t+1} = 1, \\ 5, & \text{if } B \equiv 1 \pmod 4,\ \delta_{t+1} = 1, \\ 7, & \text{if } B \equiv 3 \pmod 4,\ \delta_{t+1} = -1; \end{cases}$$

if $ab \equiv 6 \pmod 8$

$$k = \begin{cases} 1, & \text{if } B \equiv 1 \pmod 4,\ \delta_{t+1} = -1, \\ 3, & \text{if } B \equiv 3 \pmod 4,\ \delta_{t+1} = -1, \\ 5, & \text{if } B \equiv 1 \pmod 4,\ \delta_{t+1} = 1, \\ 7, & \text{if } B \equiv 3 \pmod 4,\ \delta_{t+1} = 1. \end{cases}$$

Hence we have

$$k \equiv B \pmod 4$$

and

$$\delta_t \delta_{t+1} = -\left(\frac{-2}{k}\right), \qquad \text{if } ab \equiv 0 \pmod 8,$$

$$\delta_{t+1} = \begin{cases} -\left(\frac{2}{k}\right), & \text{if } ab \equiv 2 \pmod 8, \\ -\left(\frac{-2}{k}\right), & \text{if } ab \equiv 6 \pmod 8. \end{cases}$$

Next we note that

$$\begin{aligned} &GCD\left((k-B)\left(\frac{A}{4}\right)^2+B, 2A\right) \\ &\quad = GCD\left((k-B)\left(\frac{A}{4}\right)^2+B, 8\right) GCD\left((k-B)\left(\frac{A}{4}\right)^2+B, \frac{A}{4}\right) \\ &\quad = GCD(k, 8)\, GCD\left(B, \frac{A}{4}\right) \\ &\quad = 1. \end{aligned}$$

Hence, by Dirichlet's theorem, there exist infinitely many primes $p \equiv (k-B)(A/4)^2 + B \pmod{2A}$. Choose one of these so that $GCD(p, 2ab) = 1$. Clearly we have $p \equiv B \pmod{A/4}$ and $p \equiv k \pmod 8$. As $k \equiv B \pmod 4$ we have $p \equiv B \pmod 4$ so that $p \equiv B \pmod A$. Hence, as a, b, A, B have property $(*)$, p is represented by the form $(a, 0, -b)$. As the form class $[a, 0, -b]$ belongs to the genus $\{\delta_1, ..., \delta_{t+1}\}$, we have $\chi_j(p) = \delta_j$ $(j = 1, ..., t+1)$. Thus, in particular, we have

$$\begin{aligned} \delta_t \delta_{t+1} &= \chi_t(p)\, \chi_{t+1}(p) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-2}{k}\right) \\ &= -\delta_t \delta_{t+1}, \qquad \text{if} \quad ab \equiv 0 \pmod 8, \end{aligned}$$

$$\delta_{t+1} = \begin{cases} \left(\frac{2}{p}\right) = \left(\frac{2}{k}\right) = -\delta_{t+1}, & \text{if} \quad ab \equiv 2 \pmod 8, \\ \left(\frac{-2}{p}\right) = \left(\frac{-2}{k}\right) = -\delta_{t+1}, & \text{if} \quad ab \equiv 6 \pmod 8, \end{cases}$$

which is impossible. This completes the proof of Lemma 4. ∎

LEMMA 5. *Suppose that a, b, A, B are positive integers satisfying $GCD(a, b) = GCD(A, B) = 1$, $ab \neq$ square, which possess property $(*)$. Then every genus of discriminant $4ab$ contains exactly one form class.*

Proof. Suppose that not every genus of discriminant $4ab$ contains a single form class. Since each genus contains exactly the same number of form classes, each genus must contain at least two form classes. Thus, in particular, the genus $\{\delta_1, ..., \delta_{t+1}\}$ containing the form class $[a, 0, -b]$ must also contain a form class $[u, v, w] \neq [a, 0, -b]$. Since the integers a, b, A, B possess property $(*)$, every prime $p \equiv B \pmod A$ with $GCD(p, 2ab) = 1$ is represented by the form class $[a, 0, -b]$ of the genus

$\{\delta_1, ..., \delta_{t+1}\}$, and so the arithmetic progression $\{An+B\}$ must be consistent with the values $\delta_1, ..., \delta_{t+1}$, of the generic characters $\chi_1, ..., \chi_{t+1}$. By Weber's theorem [8] the form (u, v, w) represents infinitely many primes in any arithmetic progression consistent with the generic characters of the form, that is, with the values $\delta_1, ..., \delta_{t+1}$ of $\chi_1, ..., \chi_{t+1}$. Thus we can find a prime q with $GCD(q, 2ab)=1$ in the arithmetic progression $\{An+B\}$ which is represented by (u, v, w). But, by property $(*)$, q is represented by $(a, 0, -b)$. However, as q is prime, the only form classes which can represent q are $[u, v, w]$ and $[u, -v, w]$. Since $[a, 0, -b] \neq [u, v, w]$ we must have $[a, 0, -b] = [u, -v, w]$, from which it easily follows that $[u, v, w] = [a, 0, -b]$, which is impossible. Hence every genus contains exactly one form class. ∎

COROLLARY 2. *If a, b are positive coprime integers with $ab \neq$ square and*

$$ab \equiv 1, 2, 5 \pmod 8,$$

every odd prime divisor of ab is $\equiv 1 \pmod 4$,

$$T^2 - abU^2 = -1 \text{ is insolvable in integers } T \text{ and } U,$$

and A, B are positive coprime integers, then the integers a, b, A, B do not *have property* $(*)$.

Proof. This follows immediately from Corollary 1(ii) and Lemma 5. ∎

3. PROOF OF THEOREM

We suppose that a, b, A, B are positive integers with $GCD(a, b) = GCD(A, B) = 1$, $ab \neq$ square, which possess property $(*)$. Further, by Lemma 4, we may suppose that A is even and B is odd.

Let p_0 be a prime $\equiv B \pmod A$ with $GCD(p_0, 2ab) = 1$. As a, b, A, B possess property $(*)$, p_0 is represented by the form $(a, 0, -b)$. Set $\delta_i = \chi_i(p_0)$ $(i = 1, ..., t+1)$. The form class $[a, 0, -b]$ belongs to the genus $\{\delta_1, ..., \delta_{t+1}\}$. By Lemma 5 $[a, 0, -b]$ is the only form class in the genus $\{\delta_1, ..., \delta_{t+1}\}$. Now let q be a prime $\equiv -B \pmod A$ with $GCD(q, 2ab) = 1$, so that $q \equiv -p_0 \pmod A$. Hence, by Lemma 4 we have

$$q \equiv -p_0 \pmod{2p_1 \cdots p_r}, \quad \text{if} \quad ab \equiv 1, 5 \pmod 8,$$

$$q \equiv -p_0 \pmod{4p_1 \cdots p_r}, \quad \text{if} \quad ab \equiv 3, 4, 7 \pmod 8,$$

$$q \equiv -p_0 \pmod{8p_1 \cdots p_r}, \quad \text{if} \quad ab \equiv 0, 2, 6 \pmod 8.$$

Hence for $i = 1, ..., r$ we have

$$\chi_i(q) = \left(\frac{q}{p_i}\right) = \left(\frac{-p_0}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{p_0}{p_i}\right) = (-1)^{\theta_i}\chi_i(p_0) = (-1)^{\theta_i}\delta_i.$$

If $ab \equiv 0 \pmod 8$ we have $r = t-1$ and

$$\chi_t(q) = \left(\frac{2}{q}\right) = \left(\frac{2}{-p_0}\right) = \left(\frac{2}{p_0}\right) = \chi_t(p_0) = \delta_t.$$

$$\chi_{t+1}(q) = \left(\frac{-1}{q}\right) = \left(\frac{-1}{-p_0}\right) = -\left(\frac{-1}{p_0}\right) = -\chi_{t+1}(p_0) = -\delta_{t+1}.$$

If $ab \equiv 2 \pmod 8$ we have $r = t$ and

$$\chi_{t+1}(q) = \left(\frac{2}{q}\right) = \left(\frac{2}{-p_0}\right) = \left(\frac{2}{p_0}\right) = \chi_{t+1}(p_0) = \delta_{t+1}.$$

If $ab \equiv 3, 4, 7 \pmod 8$ we have $r = t$ and

$$\chi_{t+1}(q) = \left(\frac{-1}{q}\right) = \left(\frac{-1}{-p_0}\right) = -\left(\frac{-1}{p_0}\right) = -\chi_{t+1}(p_0) = -\delta_{t+1}.$$

If $ab \equiv 6 \pmod 8$ we have $r = t$ and

$$\chi_{t+1}(q) = \left(\frac{-2}{q}\right) = \left(\frac{-2}{-p_0}\right) = -\left(\frac{-2}{p_0}\right) = -\chi_{t+1}(p_0) = -\delta_{t+1}.$$

Thus q is represented by a form class in the genus

$$\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_{t-1}}\delta_{t-1}, \delta_t, -\delta_{t+1}\}, \quad \text{if } ab \equiv 0 \pmod 8,$$

$$\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_{t+1}}\delta_{t+1}\}, \quad \text{if } ab \equiv 1, 5 \pmod 8,$$

$$\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_t}\delta_t, \delta_{t+1}\}, \quad \text{if } ab \equiv 2 \pmod 8,$$

$$\{(-1)^{\theta_1}\delta_1, ..., (-1)^{\theta_t}\delta_t, -\delta_{t+1}\}, \quad \text{if } ab \equiv 3, 4, 6, 7 \pmod 8.$$

However, by Lemmas 1 and 5, this genus contains only the form class $[-a, 0, b]$. Hence q is represented by the form $(-a, 0, b)$ completing the proof of the theorem. ∎

REFERENCES

1. B. C. BERNDT, Private communications, July 12, 1989/Sept. 13, 1989.
2. L. E. DICKSON, "Introduction to the Theory of Numbers," Dover, New York, 1957.

3. D. R. ESTES AND G. PALL, Spinor genera of binary quadratic forms, *J. Number Theory* **5** (1973), 421–432.
4. P. KAPLAN, K. S. WILLIAMS, AND Y. YAMAMOTO, An application of dihedral fields to representations of primes by binary quadratic forms, *Acta Arith.* **44** (1984), 407–413.
5. A. LEGENDRE, "Théorie des Nombres," Tome 1, Quatrième Éd., Librairie Scientifique et Technique, Albert Blanchard, Paris, 1955.
6. T. NAGELL, "Introduction to Number Theory," Almqvist & Wiksells, Stockholm, 1951.
7. S. RAMANUJAN, "Notebooks," Vols. 1 and 2, Tata Institute of Fundamental Research, Bombay, 1957.
8. H. WEBER, Beweis des Satzes, *Math. Ann.* **20** (1882), 301–329.

Printed in Belgium